UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/997,402	11/28/2001	Samir Narendra Mehta	320037.402	2381

20280 7590 09/24/2008

MOTOROLA INC
600 NORTH US HIGHWAY 45
W4 - 39Q
LIBERTYVILLE, IL 60048-5343

EXAMINER	
DOAN, DUYEN MY	

ART UNIT	PAPER NUMBER
2152	

NOTIFICATION DATE	DELIVERY MODE
09/24/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

DOCKETING.LIBERTYVILLE@MOTOROLA.COM
ADB035@Motorola.com

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Phillip Burrus on 8/20/2008.

The application has been amended as follows:

1. (Currently Amended) A method in a computer-based environment for preparing content to be deployed on a target wireless device, comprising:

determining whether pre-provisioned content corresponding to the target wireless device exists;

where the pre-provisioned content exists, determining whether the pre-provisioned content is stored with a trusted third party host, and where the pre-provisioned content is stored with the trusted third party host, retrieving the pre-provisioned content from the trusted third party host, and providing the pre-provisioned content to the target wireless device without additional provisioning; and

where the pre-provisioned content is unavailable, selecting content from remotely stored, untrusted applications and provisioning the content for the target wireless device, wherein the provisioning comprises intercepting the content and inspecting the

content, wherein the inspecting comprises at least one of examining the content to detect malicious code, determining whether the content contains banned code, and determining whether the content contains designated API;

wherein the inspecting the content comprises an operation selected from the group consisting of deconstructing a structure of the content, determining the applicable application filters, and checking a number of activated threads;

wherein the determining the applicable application of filters comprises retrieving an application filter relevant for potential targets under examination, wherein the application filter detects one of package and method names, package and method classes, package and method fields, API suspected to have intrusive behavior, API suspected to have malicious behavior and API that are unauthorized for use;

verifying that the target wireless device supports execution of the content by comparing the device capabilities to the content requirements; and providing verified and provisioned content to the target wireless device[[;]]

~~wherein the provisioning comprises inspecting the content, wherein~~ inspecting the content comprises an operation selected from the group consisting of deconstructing a structure of the content, checking for malicious code, checking for banned code, determining the applicable application of filters, and checking a number of activated threads; wherein the determining the applicable application of filters comprises retrieving an application filter relevant for potential targets under examination, wherein the application filter detects one of package and method names, package and method

classes, package and method fields, API suspected to have intrusive behavior, API suspected to have malicious behavior and API that are unauthorized for use.

6. (Currently Amended) The method of claim [[5]]1 wherein the inspecting further comprises determining whether the application contains designated API, wherein the API is at least one of packages, classes, methods, and fields.

30. (Currently Amended) (Currently Amended) A network-based transmission system operable in conjunction with at least one computer processor and memory comprising:

a provisioning manager operable to control the at least one computer processor and being configured to determine whether pre-provisioned content corresponding to a requesting device exists, and where pre-provisioned content exists, to determine whether the pre-provisioned content is stored with a trusted, third party application provider;

a deployment manager operable to control the at least one computer processor and being configured to retrieve an application, and where the pre-provisioned content is stored with the trusted, third party application provider to retrieve the pre-provisioned content from the trusted, third party application provider and to deploy the pre-provisioned content without additional provisioning, and otherwise to retrieve an application from untrusted, third party hosts; and

an inspector operable to control the at least one computer processor, wherein when the application is retrieved from an untrusted, third party host, the inspector is configured to control the at least one computer processor to examine the application by a method selected from the group consisting of examining the application to detect malicious code, performing a class analysis of the application to verify that classes in the application conform to desired standards, and applying application filters to the application;

wherein the examining comprises inspecting the content, wherein inspecting the content comprises an operation selected from the group consisting of deconstructing a structure of the content, checking for malicious code, checking for banned code, determining the applicable application of filters, and checking a number of activated threads;

wherein the determining the applicable application of filters comprises retrieving an application filter relevant for potential targets under examination, wherein the application filter detects one of package and method names, package and method classes, package and method fields, API suspected to have intrusive behavior, API suspected to have malicious behavior and API that are unauthorized for use.

45. (Currently Amended) A mobile applications system operable in conjunction with a computer processor and memory, the mobile applications system comprising

a system application operable to control a computer processor to determine

whether pre-provisioned content corresponding to a target device exists, and where it does not, prepare content for deployment on the target device, such that when the pre-provisioned content exists the computer processor determines whether the pre-provisioned content is stored with a trusted, third party application provider and fetches the pre-provisioned content from the trusted, third party application providers, and when the pre-provisioned content does not exist, to fetch a retrieved application from and untrusted, third party host;

wherein where the pre-provisioned content is stored from the trusted third party application provider, the system application is configured to deliver the pre-provisioned content without additional provisioning; and otherwise to examine the retrieved application by a method selected from the group consisting of examining the retrieved application to detect malicious code, performing a class analysis of the retrieved application to verify that classes in the retrieved application conform to desired standards, and applying application filters to the retrieved application; and

verify that the target device supports execution of the retrieved application without executing the retrieved application on the device;

wherein the examining comprises inspecting the content, wherein inspecting the content comprises an operation selected from the group consisting of deconstructing a structure of the content, checking for malicious code, checking for banned code, determining the applicable application of filters, and checking a number of activated threads;

wherein the determining the applicable application of filters comprises retrieving

an application filter relevant for potential targets under examination, wherein the application filter detects one of package and method names, package and method classes, package and method fields, API suspected to have intrusive behavior, API suspected to have malicious behavior and API that are unauthorized for use.

61. (Currently Amended) A computer-based content deployment system for one of delivering pre-provisioned content or provisioning retrieved content for a target device, operable with a computer and comprising:

a verification manager that causes the computer to verify that the retrieved content is authorized and the target device supports resources needed by the retrieved content;

a deployment manager coupled to and operational with both the verification manager and the computer, the deployment manager configured to retrieve content from at least trusted, third party application providers, and untrusted, third party hosts; an inspector, coupled to and operational with the verification manager and deployment manager and the computer, wherein when the content is retrieved from an untrusted, third party host, the inspector examines the retrieved content by a method selected from the group consisting of examining the retrieved content to detect malicious code, performing a class analysis of the retrieved content to verify that classes in the retrieved content conform to desired standards, and applying application filters to the retrieved content; and

a provisioning manager, operable with the computer, and operable with and coupled to the verification manager, the deployment manager and the inspector, that, where the content is retrieved from one or more of the untrusted, third party hosts, provisions the retrieved content according to requirements of the target device by at least one of inspecting the content, optimizing the content, and instrumenting the content, or determines whether pre-provisioned content exists, and where the pre-provisioned content exists, determines whether the pre-provisioned content is stored with a trusted, third party host, and where the pre-provisioned content is stored with the trusted third party host, retrieves the pre-provisioned content from the trusted third party host without additional provisioning; wherein inspecting the content comprises an operation selected from the group consisting of deconstructing a structure of the content, checking for malicious code, checking for banned code, determining the applicable application of filters, and checking a number of activated threads; wherein the determining the applicable application of filters comprises retrieving an application filter relevant for potential targets under examination, wherein the application filter detects one of package and method names, package and method classes, package and method fields, API suspected to have intrusive behavior, API suspected to have malicious behavior and API that are unauthorized for use.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DUYEN M. DOAN whose telephone number is (571)272-4226. The examiner can normally be reached on 9:30am-6:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Bunjob Jaroenchonwanit can be reached on (571) 272-3913. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Bunjob Jaroenchonwanit/

Supervisory Patent Examiner, Art Unit 2152